



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

BB

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,239	09/12/2003	David D. Brandt	03AB014A/ALBRP303USA	6849
7590	12/15/2005		EXAMINER	
Susan M. Donahue Rockwell Automation 704-P, IP Department 1201 South 2nd Street Milwaukee, WI 53204			PHAM, THOMAS K	
			ART UNIT	PAPER NUMBER
			2121	
			DATE MAILED: 12/15/2005	

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	10/661,239	BRANDT ET AL.	
	Examiner	Art Unit	
	Thomas K. Pham	2121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 12 September 2003.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-33 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-33 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 12 September 2003 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.  
 5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_\_.

**First Action on the Merits**

1. Claims 1-33 of U.S. Application 10/661,239 filed on 09/12/2003 are presented for examination.

**Quotations of U.S. Code Title 35**

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

***Claim Rejections - 35 USC § 101***

6. The language of the claim raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claims 1-8 and 11-19 are rejected under 35 U.S.C. 101 as not being tangible since the elements or features of the claimed Machine can be implemented by software alone. For example, the term “an automation security system” can be interpreted as a security software or program for use in an automation environment, wherein the software includes components such as an asset component, access component and a security component. The system as claimed represents a functional software for an automation environment that is not embodied in a manner so as to be executable.

Claim 24-27 are is rejected under 35 U.S.C. 101 as not being tangible since the steps of the method do not require use of hardware or computer system to accomplish the steps. For example, any person can analyze the assets, modeling the assets according to a security concern, and then develop a security plan based on the model and type of network. There is no practical application asserted in the claims.

Claims 29-33 are rejected under 35 U.S.C. 101 as not being tangible since the elements or features of the claimed Machine can be implemented by software alone. For example, the security schema is interpret as a set of software objects (e.g. tables, views, indexes, etc.) or a description of data represented within a structure database. The schema as claimed represents a

functional software for a database data structure that is not embodied in a manner so as to be executable.

### **Claim Rejections - 35 USC § 102**

7. Claims 1-7 and 11-33 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,571,141 (“Brown”).

#### **Regarding claim 1**

Brown teaches an automation security system, comprising:

- an asset component to define one or more factory assets (see col. 4 lines 53-57);
- an access component to define one or more security attributes associated with the factory assets (see col. 7 lines 48-59); and
- a security component to regulate access to the factory assets based upon the one or more security attributes (see col. 6 lines 41-56).

#### **Regarding claim 20**

Brown teaches an automation security system, comprising:

- one or more servers that manage a network interface between networked factory assets (see col. 4 lines 26-39) and other devices or users attempting access to the networked factory assets (see col. 4 lines 53-57); and
- a security management module associated with the network interface for enforcing an enterprise wide policy and to manage security threats directed to the networked factory assets (see col. 6 lines 41-56).

#### **Regarding claim 24**

Brown teaches an automation security methodology, comprising:

- analyzing one or more automation assets (see col. 4 lines 53-57);
- modeling the automation assets in accordance with network security considerations (see col. 7 lines 48-59); and
- developing a security framework for an automation system based in part on the modeling of the automation assets and a network access type (see col. 6 lines 41-56).

**Regarding claim 28**

Brown teaches an automated security system for an industrial control environment, comprising:

- means for defining one or more security attributes associated with at least one network request (see col. 7 lines 48-59);
- means for processing the one or more security attributes (see col. 9 lines 30-38); and
- means for controlling access to at least one of a network device and an automation component based in part on the one or more security attributes (see col. 6 lines 41-56).

**Regarding claim 29**

Brown teaches a security schema for a factory automation system, comprising:

- a first data field to describe factory assets (see col. 4 lines 53-57);
- a second data field to describe security parameters for the factory assets (see col. 7 lines 21-34); and
- a schema to associate the first and second data fields, the schema employed to limit access to the factory assets based upon the security parameters (see col. 7 lines 35-47).

**Regarding claim 2**

Brown teaches the one or more or more security attributes including at least one of a role attribute, a time attribute, a location attribute, and an access type attribute (see col. 10 lines 33-40, “security level”).

**Regarding claim 3**

Brown teaches the security component is based on at least one of a formal threat analysis, a vulnerability analysis, a factory topology mapping and an attack tree analysis (see col. 10 lines 20-32).

**Regarding claim 4**

Brown teaches the security component is based on at least one of automation and process control security, cryptography, and Authentication/Authorization/Accounting (AAA) (see col. 6 lines 6-10).

**Regarding claim 5**

Brown teaches the asset component describes at least one of factory components and groupings, the factory components are at least one of sensors, actuators, controllers, I/O modules, communications modules, and human-machine interface (HMI) devices (see col. 4 lines 12-25, “controller”).

**Regarding claim 6**

Brown teaches the groupings include factory components that are grouped into at least one of machines, machines grouped into lines, and lines grouped into facilities (see col. 4 lines 53-57).

**Regarding claim 7**

Brown teaches the groupings have associated severity attributes such as at least one of risk and security incident cost (see col. 6 lines 57-67).

**Regarding claim 11**

Brown teaches security parameters and policies that are developed for physical and electronic security for various component types (see col. 4 lines 47-61).

**Regarding claim 12**

Brown teaches the security parameters and policies further comprising at least one of security protection levels, identification entry capabilities, integrity algorithms, and privacy algorithms (see col. 9 lines 30-37).

**Regarding claim 13**

Brown teaches the security component includes at least one of authentication software, virus detection, intrusion detection, authorization software, attack detection, protocol checker, and encryption software (see col. 10 lines 33-40).

**Regarding claim 14**

Brown teaches the security component at least one of acts as an intermediary between an access system and one or more automation components, and facilitates communications between the access system and the one or more automation components (see col. 10 lines 11-19).

**Regarding claim 15**

Brown teaches the security attributes are specified as part of a network request to gain access to the one or more factory assets, the security attributes included in at least one of a group, set, subset, and class (see col. 9 lines 9-18).

**Regarding claim 16**

Brown teaches the security component employs at least one authentication procedure and an authorization procedure to process the network request (see col. 9 line 66 to col. 10 line 10)

**Regarding claim 17**

Brown teaches one or more security protocols including at least one of Internet Protocol Security (IPSec), Kerberos, Diffie-Hellman exchange, Internet Key Exchange (IKE), digital certificate, pre-shared key, and encrypted password, to process the network request (see col. 9 lines 30-36, “password”).

**Regarding claim 18**

Brown teaches at least one of an access key and a security switch to control network access to a device or network (see col. 10 lines 20-32, “security mask”).

**Regarding claim 19**

Brown teaches the access key further comprises at least one of time, location, batch, process, program, calendar, GPS (Global Positioning Information) to specify local and wireless network locations, to control access to the device or network (see col. 10 lines 33-40, “API function”).

**Regarding claim 21**

Brown teaches the security management module at least one of schedules audits, establishes a security policy, applies the policy from a single or distributed console, and generates reports that identify potential weaknesses in security (see col. 7 lines 21-34, “restricted parameters”).

**Regarding claim 22**

Brown teaches the security management module provides an interface to at least one of add, delete and modify security rights of an individual, a group, or a device and distribute security

information to various controllers and control devices (see col. 9 lines 39-47, “alter the settings of security system”).

**Regarding claim 23**

Brown teaches further comprising at least one of: an authentication with the one or more servers to establish a secure link; a secure link to authenticate and authorize access to a requestor of the networked factory assets; and establishment of a secure session with the requestor if access is authorized (see col. 10 lines 34-40).

**Regarding claim 25**

Brown teaches analyzing one or more security attributes to determine whether access should be granted to the one or more automation assets (see col. 10 lines 6-32).

**Regarding claim 26**

Brown teaches the one or more security attributes further comprise at least one of a role, an asset type, a location, a time, and an access type (see col. 10 lines 33-40).

**Regarding claim 27**

Brown teaches at least one of: determining whether to grant access to the one or more automation assets; granting access from the one or more automation assets; and granting access from a network device associated with the one or more automation assets (see col. 10 lines 6-32).

**Regarding claim 30**

Brown teaches the schema including at least one of an access role, an asset type, an access type, time information, address information, and location information (see col. 10 lines 33-40).

**Regarding claim 31**

Brown teaches a response schema to provide status to a requesting network device (see col. 10 lines 25-32, “ACCESSDENIED”).

**Regarding claim 32**

Brown teaches the response schema including at least one of a status field, a time field, an access type field, an access location field, and a key field (see col. 10 lines 25-32, “defining the access rights”).

**Regarding claim 33**

Brown teaches the response schema including an attachment field to indicate other security data follows the response schema (see col. 10 lines 25-32).

**Claim Rejections - 35 USC § 103**

8. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,571,141 (“Brown”).

**Regarding claim 8**

Brown does not specifically teach an ISA S95 Model for Enterprise to Control System integration to integrate security aspects across or within respective groupings. “Official Notice” is taken that both the concept and advantages of providing an ISA S95 Model for Enterprise to Control System integration to integrate security aspects across or within respective groupings is well known and expected in the art. U.S. Patent Application Publication No. 2003/0014500 to Schleiss et al. discloses a preferred flow of communication between various process control and information technology systems are typically found within an enterprise defined by an ISA S95 model international standard (see paragraphs 7 and 8). It would have been obvious to one of

ordinary skill in the art to include the ISA S95 model for Enterprise to Control System because it would provide for interacting between production or process control systems, enterprise resource planning systems and manufacturing execution systems to facilitate the integration of these systems.

9. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,571,141 (“Brown”) in view of U.S. Patent Application Publication 2002/0006790 A1 (“Blumenstock”).

**Regarding claim 9**

Brown does not specifically teach a set of generic IT components and specifies parameters to assemble and configure the IT components to achieve flexible access to the one or more factory assets.

However, Blumenstock teaches a set of generic IT components for providing remote maintenance and/or diagnostic with a flexible access using an encryption device at transmitting server and a decryption device at a remote server (see paragraphs 14 and 15) for the purpose of preventing unauthorized penetration of a firewall to the automation system (see paragraph 8).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the flexible access of Blumenstock with the system of Brown because it would provide for the purpose of preventing unauthorized penetration of a firewall to the automation system.

**Regarding claim 10**

Blumenstock teaches the IT components include at least one of switches with virtual local area network (VLAN) capability, routers with access list capability, firewalls, virtual private network (VPN) termination devices, intrusion detection systems, AAA servers, configuration tools, and monitoring tools (see paragraph 8, “firewall”).

***Conclusion***

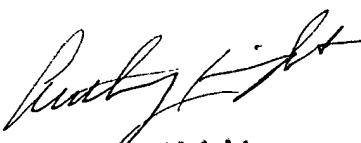
Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner *Thomas Pham*; whose telephone number is (571) 272-3689, Monday - Thursday from 6:30 AM - 5:00 PM EST or contact Supervisor *Mr. Anthony Knight* at (571) 272-3687.

Any response to this office action should be mailed to: **Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.** Responses may also be faxed to the **official fax number (571) 273-8300.**

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

**Thomas Pham**  
*Patent Examiner*

December 8, 2005



**Anthony Knight**  
*Supervisory Patent Examiner*  
Group 3600